音楽配信サービスMOOCSにおけるセキュリティ技術　MQbic$_{TM}$

MQbic$_{TM}$ Content Protection Technology Adopted for MOOCS Service

野口　正典　■ NOGUCHI Masanori
松川　伸一　■ MATSUKAWA Shinichi
海谷　一浩　■ KAIYA Kazuhiro

デジタルコンテンツ配信の普及により，ユーザーの利便性を保ったうえでコンテンツホルダーの権利を守るコンテンツ保護技術 DRM (Digital Rights Management) が求められている。

東芝ソリューション (株) は，東芝と共同でSDメモリカードを使用するコンテンツ保護技術 MQbic$_{TM}$ (マルチキュービック) を開発し，これらの両立を実現した。MQbic$_{TM}$は，ニフティ (株) の音楽コンテンツ配信サービス MOOCS(注1) (ムークス) のDRMとして採用されている。

Accompanying the widespread dissemination of digital content delivery, there is a strong need for digital rights management (DRM) technology to protect copyrights while maintaining the users' convenience. Toshiba Solutions Corporation and Toshiba collaborated to develop MQbic$_{TM}$, a DRM technology that utilizes the secure digital (SD) memory card and achieves the ideal balance between users' convenience and copyright protection. MQbic$_{TM}$ is employed as the DRM technology for the MOOCS electronic music distribution service operated by NIFTY Corporation.

1　まえがき

近年，インターネットの常時接続が一般家庭に普及したことにより，デジタルコンテンツ配信市場への注目が高まっている。音楽コンテンツの楽しみ方としては，ユーザーがCDなどのパッケージメディアを購入して家庭内で再生したり，テープやMD (ミニディスク) などの媒体へ記録して屋外で視聴するという形態が中心であった。

しかし最近では，デジタルコンテンツとしてパソコン (PC) などへ取り込んだり，フラッシュメモリ及びハードディスク装置 (HDD) 内蔵の携帯音楽プレーヤを屋外で利用する形態が主流になりつつある。その背景には，携帯音楽プレーヤの普及に見られるように，ユーザー側で配信を受けられる環境が整いつつあることが挙げられる。この市場の拡大に伴い，ISP (Internet Service Provider) による音楽コンテンツ配信サービスへの取組みが活発化してきている。

一方では，P2P (Peer to Peer) を利用したファイル共有アプリケーションによるコンテンツの違法コピーが横行し，「コンテンツホルダーの権利をいかに守るか」という問題も同時に発生している。このため，コンテンツホルダーの権利を保護する技術が重要視されている。

しかし，コンテンツ保護を重視するあまり再生できる環境を限定してしまうと，ユーザーの利便性が損なわれてしまう。したがって，コンテンツホルダーの権利を保護したうえでユーザーの利便性を損なわないような，特定の機器に縛られないコンテンツ保護技術が求められている。

その解決策として，東芝ソリューション (株) は東芝と共同でコンテンツ保護技術 MQbic$_{TM}$ (マルチキュービック) を開発し，ニフティ (株) の音楽配信サービス MOOCS (ムークス) に採用された。

ここでは，ユーザーの利便性とコンテンツ保護を両立したMQbic$_{TM}$の概要について述べる。

(注1)　MOOCSは，ニフティ株式会社の登録商標である。

2　MQbic$_{TM}$の概要

MQbic$_{TM}$は，次の三つのマルチをセキュアに実現することをコンセプトとしている。

(1)　Multi Content (多様なコンテンツを)
(2)　Multi Distribution (多様な配信方式で)
(3)　Multi Terminal (多様な端末に)

MQbic$_{TM}$は，デジタルコンテンツの配信の保護にSD-DRM (Separate Delivery-Digital Rights Management) を，また，SDメモリカードに記録されたコンテンツの保護に，記録メディアのコンテンツ保護技術の一つであるCPRM (Content Protection for Recordable Media) を採用している (**図1**)。

配信されるデジタルコンテンツは，暗号化コンテンツと再生する権利とに分かれている。再生する権利には，対応するコンテンツの暗号・復号に使われる鍵と，コピー回数などの利用ルールが含まれる。コンテンツや鍵のフォーマットは，SDメモリカードの規格策定を行うSD Card Association(1)のSD-SD

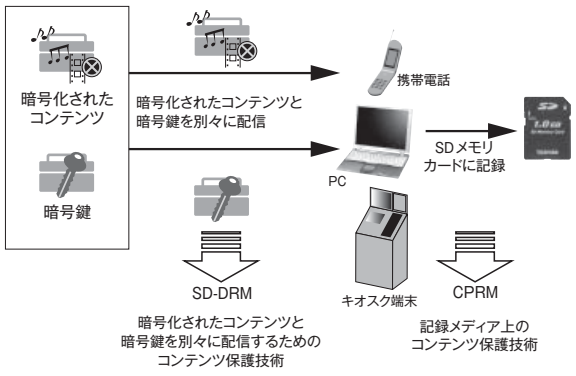

図1. MQbic$_{TM}$の概要 ― コンテンツ配信の保護技術にSD-DRM，SDメモリカードでのコンテンツ保護にCPRMを採用している。
Overview of fields of application for MQbic$_{TM}$

(Secure Digital-Separate Delivery) 規格をベースに構築されている。

SD-DRMとCPRMのコンテンツ保護の仕組みについては5章で説明する。

3　MQbic$_{TM}$の特長

MQbic$_{TM}$は，次の三つの特長を備えており，これらの特長が評価され，ニフティ(株) が提供する音楽コンテンツ配信サービス　MOOCSのDRMとして採用されている。

(1)　認知度が高いコンテンツ保護方式
(2)　超流通の実現
(3)　SD-Audioに対応

MOOCSでは，音楽コンテンツの購入をPCで行い，再生はPC又は携帯機器などSD-Audioに対応した機器で行うことを想定している。

3.1　認知度が高いコンテンツ保護方式

MQbic$_{TM}$の記録メディア上のコンテンツ保護方式は，SDメモリカードやDVD記録メディア (DVD-Rなど) で採用されているCPRMをベースに構築されている。CPRMは，IBM社，Intel社，松下電器産業 (株)，及び東芝が設立した団体である4C Entity，LLC[(2)]が策定した規格である。暗号アルゴリズムに松下電器産業 (株) と東芝が開発したC2を採用しており，不正機器排除機能などを備えている。CPRMは，携帯電話のSDメモリカードに保存されるデジタルコンテンツの保護や，日本の地上・BS・CSデジタル放送の録画方式の一つとしても採用実績がある。

コンテンツ配信サービス事業者がコンテンツの売買契約を行う際に，スタジオや音楽レーベルなどのコンテンツホルダーへ著作権保護技術の説明を行うが，MQbicはコンテンツホルダーの認知度が高く，かつ実績のあるCPRMがベースになっていることで理解を得やすい。

3.2　超流通の実現

コンテンツと権利を分離して流通させる“超流通”(Separate Delivery) を，PC上でセキュアに実現している。

MQbic$_{TM}$を採用した配信システムでは，暗号化したコンテンツを自由に流通・配布し，再生したいときにコンテンツの復号鍵を購入してPCに保存できるようになる。また，SD-SD 規格の中のAudio Profile (SD-SD Audio) にも対応しているため，コンテンツの復号鍵をSDメモリカードに，また，暗号化したコンテンツをCDやPCのHDDなど別の記録媒体に，分けて記録することもできる。

例えば，SD-SD Audio形式で保存したコンテンツをインターネットや雑誌の付録として配布し，ユーザーは再生したいコンテンツの権利を後から購入してSDメモリカードに保存することができる。

3.3　SD-Audioに対応

MQbic$_{TM}$は，音楽コンテンツをSDメモリカードへ記録するときに，SDメモリカードの標準アプリケーションフォーマットであるSD-Audio形式で書き込む。このため，SD-Audioに対応した携帯電話や携帯音楽プレーヤなどで音楽を聴くことができる。

4　“再生する権利”のメディアへの記録

コンテンツ保護における課題として，“コンテンツデータの保護”と“機器バインド”の二つが考えられる。コンテンツデータの保護とは，コンテンツデータが第三者により読み出され，著作権の侵害など不正に利用されるのを防ぐことである。機器バインドとは，コンテンツが記録された端末 (PC，携帯音楽プレーヤ，携帯電話など) 以外の，コンテンツホルダーが想定していない機器やメディアへの出力又はコピーを防ぐことである。

多くのサービスでは，複数の端末やメディア間でのコンテンツの移動及びコピーを制限している。このため，例えば，家庭内のPCでダウンロードしたコンテンツを外出先のPC又はカーナビなどで再生することができず，ユーザー側の利便性が損なわれている。

MQbic$_{TM}$は，PC上のコンテンツの“再生する権利”だけをPCのHDD又はSDメモリカードなどの記録媒体にバインドし保護して記録する。コンテンツデータは暗号化されて別の媒体に記録することができる。この再生する権利と暗号化コンテンツデータの組合せで再生が可能となる。

暗号化コンテンツデータそのものは，インターネットでの送信や媒体への記録を無制限に行うことができるが，再生する権利がないと，暗号化コンテンツデータそのものは再生できない。この再生する権利をSDメモリカードなど保護されたメディアで持ち運ぶことで，課題であった利便性を向上させることができる。

5　コンテンツ保護の仕組み

前に述べたように，デジタルコンテンツ配信サービスを構築するにあたり，コンテンツ保護の仕組みが重要になってくる。これは，不正に音楽コンテンツをコピーして配布できないようにするためである。MQbic$_{TM}$では，図1に示したように，コンテンツの配信にはSD-DRMを，また，SDメモリカード上ではCPRMを使用してコンテンツ保護を実現している。

5.1　SD-DRM

SD-DRMは，暗号化されたコンテンツと，このコンテンツを復号するための鍵（以下，コンテンツ鍵と略記）を別々に配信（超流通）するためのコンテンツ保護技術である。

MQbic$_{TM}$は，コンテンツ鍵をSDメモリカードに保存するSD-SD Audioにも対応している。執筆時点でSD-SD Audioに対応した端末がなかったため，ここではコンテンツ鍵をPCに保存するSD-DRMについて説明する（**図2**）。

SD-DRMでは，コンテンツ本体をタイトルや再生時間などのコンテンツ情報とともにコンテンツ鍵で暗号化し，MQbic$_{TM}$対応プレーヤへ配信する。配信時に第三者が入手しても，コンテンツ鍵がないため再生できない。コンテンツの暗号化には，後述するCPRMで採用されている暗号・復号アルゴリズムのC2暗号が利用されている。

コンテンツ鍵は，ユーザーがコンテンツを再生する権利を購入したときにMQbic$_{TM}$対応プレーヤへ配信される。コンテンツ鍵も配信時にはユーザー鍵で暗号化されているので，第三者が入手しても再生することができない。

ユーザー鍵は，あらかじめMQbic$_{TM}$対応プレーヤに個別に配布される暗号・復号鍵で暗号化されて，配信される。MQbic$_{TM}$対応プレーヤは，このユーザー鍵を使用して，暗号化されたコンテンツ鍵を復号し，コンテンツを復号・再生することができる。

また，暗号化されたコンテンツ鍵を配信するときに，コンテンツのコピー可能回数やCDへの書込み可否などの使用ルールを付加することが可能である。この使用ルールをUsage Ruleと呼ぶ。

MQbic$_{TM}$では，暗号化されたコンテンツ鍵の配信時にUsage Ruleを生成している。このため，同じコンテンツに対して動的にUsage Ruleを変えることができる。

Usage Ruleには，コンテンツの再生が可能な期間や時間を設定することができる。例えば，レンタルCDのような1週間だけの再生を許可するビジネスモデルに利用できる。新しいコンテンツは2日間，古いコンテンツは1週間とするなど再生期間に差をつけることや，キャンペーン期間だけ再生を許可するといった，きめ細かな設定を行うこともできる。

5.2　SDメモリカードのCPRM

コンテンツは記録メディア上に暗号化されて記録され，この暗号を復号するタイトル鍵はコンテンツ本体とは分けて記録される。タイトル鍵は，記録メディア1枚1枚が持つ固有情報とデバイス鍵を元に生成されるメディア固有鍵で暗号化され，保護領域に記録される（**図3**）。ここでの暗号化はC2暗号を利用している。保護領域へアクセスするには，SDメモリカードとの認証処理が必要で，デバイス鍵を持たない機器はアクセスすることができない。

一方，暗号化されたコンテンツは，SDメモリカードのユーザーデータエリアに記録されるため，ユーザーが自由にアクセスすることが可能である。ユーザーが暗号化コンテンツをほ

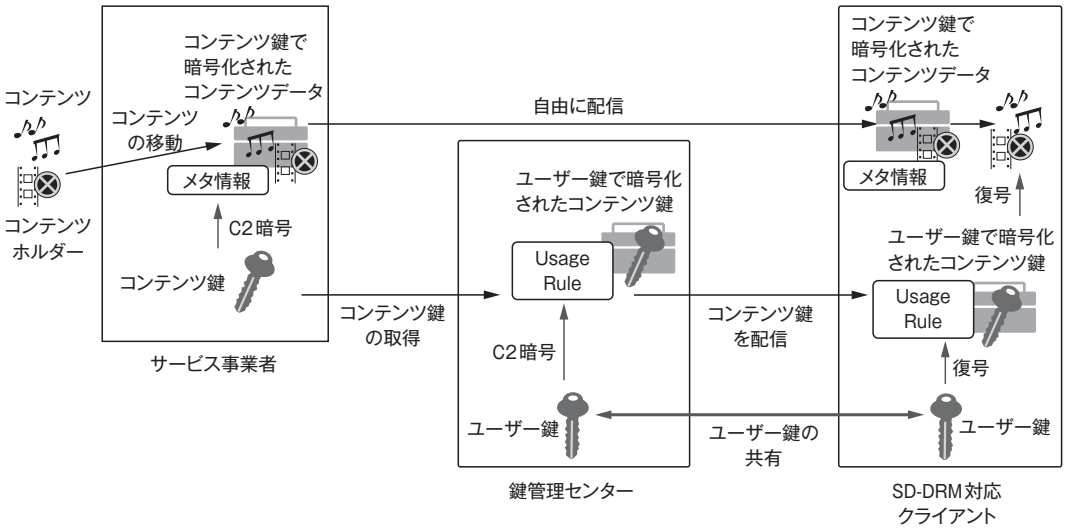

図2．SD-DRMの概要 ― 暗号化されたコンテンツとコンテンツ鍵は別々に配信され，PCに保存される。
Data flow of separate delivery (SD)-DRM

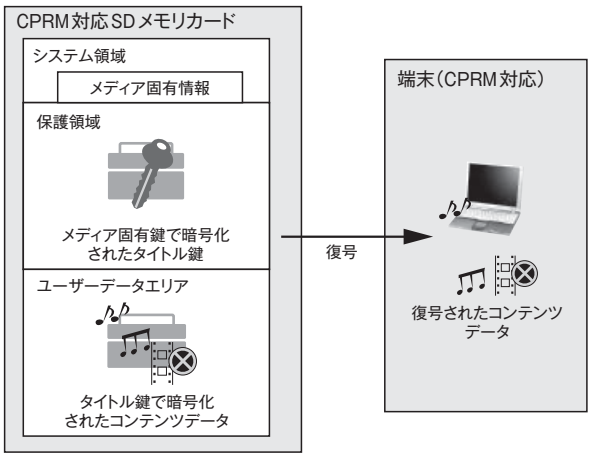

図3．SD-AudioにおけるCPRMの構成 ― コンテンツはタイトル鍵とメディア固有鍵で2段に暗号化されている。

Configuration of content protection for recordable media (CPRM)

かの記録メディアにコピーしても，復号するためのタイトル鍵がコピーできないため，再生することができない。

MQbic$_{TM}$は，SDメモリカードへのコンテンツ書込みにこのCPRMを採用したSD-Audioフォーマットで記録する。このため，SD-Audioに対応した携帯電話やミニコンポなど市販されている多くの機器でコンテンツを再生することができる。

6　デジタルコンテンツ配信システムの概念

MQbic$_{TM}$を使用した，デジタルコンテンツ配信システムの概要を**図4**に示す。

ユーザーは，PCを使用して配信サービス事業者のWebサイトからコンテンツを購入すると，配信サービス事業者経由で鍵管理センターから暗号化されたコンテンツ鍵を入手することができる。

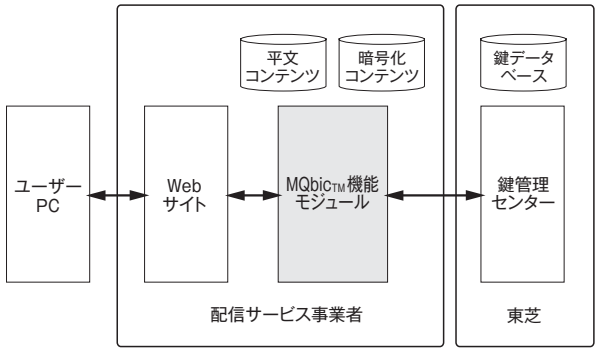

図4．デジタルコンテンツ配信システムの概要 ― MQbic$_{TM}$機能モジュールは，配信サービス事業者のシステムに組み込まれる。

MQbic$_{TM}$ in content delivery system

鍵管理センターは東芝が運用・管理し，配信サービス事業者に対してコンテンツ保護に使用するユーザー鍵やコンテンツ鍵などの鍵情報を提供している。

MQbic$_{TM}$を実現するためのモジュールは，配信サービス事業者のシステムに組み込まれ，次の機能を提供する。

(1)　コンテンツ暗号化機能　　コンテンツ鍵で平文コンテンツを暗号化

(2)　ユーザー鍵配信機能　　鍵管理センターが発行するユーザー鍵を配信

(3)　暗号化コンテンツ鍵配信機能　　暗号化されたコンテンツ鍵をMQbic$_{TM}$対応プレーヤに配信。主にコンテンツ購入の際に使用

7　あとがき

コンテンツ保護技術であるMQbic$_{TM}$は，コンテンツの鍵を保護する技術が中核にある。したがって，音楽だけではなく，動画や書籍などのコンテンツにも適用できる。最新の携帯音楽プレーヤや携帯電話では，ワンセグ放送や電子書籍への対応も進んでいるので，今後，音楽以外のコンテンツ配信市場へもMQbic$_{TM}$の適用を進めていきたい。

文　献

(1)　SD Card Association. SD Card Associationホームページ. ＜http://www.sdcard.org/＞,（参照2007-05-10）.

(2)　4C Entity, LLC. 4C Entityホームページ. ＜http://www.4centity.com/＞,（参照2007-05-10）.

野口　正典　NOGUCHI Masanori

東芝ソリューション（株）エンベデッドソリューション事業部企画部主任。コンテンツセキュリティシステムの開発に従事。

Toshiba Solutions Corp.

松川　伸一　MATSUKAWA Shinichi

東芝ソリューション（株）IT技術研究所 研究開発部。コンテンツセキュリティの規格策定，要素技術開発，及びソフトウェア技術開発に従事。

Toshiba Solutions Corp.

海谷　一浩　KAIYA Kazuhiro

東芝ソリューション（株）エンベデッドソリューション事業部モバイルコンピューティング技術部主任。コンテンツセキュリティシステムの開発に従事。

Toshiba Solutions Corp.